IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

K.L., an individual; on behalf of herself and all others similarly situated,

Plaintiff,

v.

LEGACY HEALTH, an Oregon nonprofit healthcare provider,

Defendant.

Case No. 3:23-cv-1886-SI

OPINION AND ORDER

Timothy S. DeJong, STOLL STOLL BERNE LOKTING & SHLACHTER, PC, 209 SW Oak Street, Suite 500, Portland, OR 97204; Joseph M. Lyon, Clint Watson, THE LYON FIRM, 2754 Erie Avenue, Cincinnati, OH 45208; Gary M. Klinger, MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC, 227 W. Monroe Street, Suite 2100, Chicago, IL 60606; Glen L. Abramson, MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC, 800 S. Gay Street, Suite 1100, Knoxville, TN 37929; Philip Joseph Krzeski, CHESTNUT CAMBRONNE PA, 100 Washington Avenue South Suite 1700, Minneapolis, MN 55401; Terence Coates, Dylan J. Gould, MARKOVITS, STOCK & DEMARCO, LLC, 119 East Court Street, Suite 530, Cincinnati, OH 45202. Of Attorneys for Plaintiff.

Curt Roy Hineline, Alexander Vitruk, BAKER & HOSTETLER LLP, 999 Third Avenue, Suite 3900, Seattle, WA 98104; Dyanne J. Cho, Teresa Carey Chow, BAKER & HOSTETLER LLP, 1900 Avenue of the Stars, Suite 2700, Los Angeles, CA 90067-4508; Paul G. Karlsgodt, BAKER & HOSTETLER LLP, 1801 California Street, Suite 4400, Denver, CO 80202. Of Attorneys for Defendant.

Michael H. Simon, District Judge.

Plaintiff K.L. brings this putative class action against her healthcare provider, Defendant Legacy Health, on behalf of herself and other similarly situated Legacy patients. She alleges that Defendant installed data tracking tools on its website, allowing Meta Platforms, Inc. d/b/a Meta ("Meta")[1] and Alphabet, Inc. d/b/a Google ("Google"),[2] to improperly access Plaintiff's confidential personally identifiable information and protected health information ("PHI") without her knowledge or consent. Plaintiff alleges six claims: (1) breach of confidence; (2) violation of the Electronic Communications Privacy Act ("ECPA"); (3) intrusion upon seclusion; (4) breach of implied contract; (5) unjust enrichment; and (6) negligence. Defendant moves to dismiss all six claims under Rule 12(b)(6) of the Federal Rules of Civil Procedure. For the reasons discussed below, the Court grants in part and denies in part Defendant's motion.

STANDARDS

A motion to dismiss for failure to state a claim may be granted only when there is no cognizable legal theory to support the claim or when the complaint lacks sufficient factual allegations to state a facially plausible claim for relief. *Shroyer v. New Cingular Wireless Servs., Inc.*, 622 F.3d 1035, 1041 (9th Cir. 2010). In evaluating the sufficiency of a complaint's factual allegations, the court must accept as true all well-pleaded material facts alleged in the complaint

[1] Plaintiff refers to Meta as Facebook in her complaint. Meta rebranded its corporate entity from Facebook in 2021, and the Court refers to it as Meta.

[2] Plaintiff describes the tracking tools as belonging to "Facebook" and "Google, Inc.," but Facebook rebranded its corporate entity to Meta in 2021 and Alphabet, Inc. replaced Google, Inc. as the publicly traded entity in 2015. Google, Inc. is not an active company, although Google LLC is an active company, a subsidiary of Alphabet, Inc. that focuses on online search and advertising services. It is unclear whether Plaintiffs meant to reference Alphabet, Inc. or Google, LLC. For purposes of this motion, it is not material and the Court considers that Plaintiff meant to reference Alphabet, Inc.

and construe them in the light most favorable to the non-moving party. *Wilson v. Hewlett-Packard Co.*, 668 F.3d 1136, 1140 (9th Cir. 2012); *Daniels-Hall v. Nat'l Educ. Ass'n*, 629 F.3d 992, 998 (9th Cir. 2010). To be entitled to a presumption of truth, allegations in a complaint "may not simply recite the elements of a cause of action, but must contain sufficient allegations of underlying facts to give fair notice and to enable the opposing party to defend itself effectively." *Starr v. Baca*, 652 F.3d 1202, 1216 (9th Cir. 2011). The court must draw all reasonable inferences from the factual allegations in favor of the plaintiff. *Newcal Indus. v. Ikon Off. Sol.*, 513 F.3d 1038, 1043 n.2 (9th Cir. 2008). The court need not, however, credit a plaintiff's legal conclusions that are couched as factual allegations. *Ashcroft v. Iqbal*, 556 U.S. 662, 678-79 (2009).

A complaint must contain sufficient factual allegations to "plausibly suggest an entitlement to relief, such that it is not unfair to require the opposing party to be subjected to the expense of discovery and continued litigation." *Starr*, 652 F.3d at 1216. "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678 (citing *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 556 (2007)). "The plausibility standard is not akin to a probability requirement, but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Mashiri v. Epsten Grinnell & Howell*, 845 F.3d 984, 988 (9th Cir. 2017) (quotation marks omitted).

BACKGROUND

A. Plaintiff K.L.'s Allegations

Plaintiff has been a patient of Defendant Legacy Health since 2014. Compl. (ECF 1) ¶ 93. She alleges that she regularly used Defendant's services for physical therapy and primary care. *Id.* ¶ 96. In 2022, she sought treatment from Defendant's burn unit to treat burn wounds. *Id.* To

that end, Plaintiff frequently visited two different parts of Defendant's website: Defendant's public facing website ("Public Website") and her MyHealth patient portal ("Patient Portal"). *Id.* ¶¶ 97-99. The Public Website is accessible to patients and nonpatients alike, who can use the website to browse Defendant's services or research medical conditions. *See id.* ¶¶ 97, 99. Plaintiff used the Public Website to research burn wound treatments and find contact information for burn specialists at Legacy. *Id.* The Patient Portal is a personalized, password protected page; Legacy patients may register for a Patient Portal to communicate online with their physicians, retrieve healthcare records, review prescriptions, sign up for research, and schedule appointments. *See id.* ¶¶ 98-99. Plaintiff used her Patient Portal for all of those reasons. *Id.*

Plaintiff alleges that at some point "[a]fter searching for burn specialists on Defendant's Website[3] and receiving burn treatments from Defendant's specialists," she began to see on her Facebook page advertisements related to medical supplies for burns, vitamins to promote burn healing, and exercises for burns. *Id.* ¶ 111. Plaintiff further alleges that she found tracking tools of Meta and Google on both the Public Website and the Patient Portal. *Id.* ¶¶ 55, 71, 104. Tracking tools are software that website operators can integrate into their websites to collect and analyze user activity.[4] *Id.* ¶ 44. By collecting this data, tracking tools help target and market products to a website's users. *Id.* ¶ 46. Based on their activity on a website that hosts tracking tools, users may receive advertisements on *other* websites, such as their Facebook pages. In this case, Plaintiff alleges that when she looked at the coded structure of the Public Website—which

[3] During oral argument, Plaintiff's counsel clarified that Plaintiff conducted these searches on *both* the Public Website and the Patient Portal.

[4] Plaintiff provides detailed allegations regarding how internet source code and tracking tools generally work. *See* Compl. ¶¶ 34-53. She also provides detailed allegations regarding the alleged tracking tools on Defendant's website, including screenshots. *Id.* ¶¶ 54-92.

is not automatically visible when someone visits the website—she saw two tracking tools, Google Analytics and Meta Pixel. *See id.* ¶¶ 54, 71-72, 75. She also alleges that she could see that Google Analytics was running *within* the Patient Portal as well.[5] *See id.* ¶¶ 88, 91, 104.

Plaintiff further alleges that she never disclosed information about her burns anywhere else on the internet (for example, directly into a Google search) beyond Defendant's Public Website and her Patient Portal. *Id.* ¶¶ 111-12. Thus, Plaintiff claims, Defendant must have unlawfully disclosed her data—including her health information protected by federal statute—to Meta and Google by embedding the Meta Pixel and Google Analytics tracking technology on its websites. *Id.* Based on these allegations, Plaintiff brings the six claims described above on behalf of herself and a putative class of similarly situated individuals.[6]

B. The Health Insurance Portability and Accountability Act

In 1996, Congress enacted The Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C. § 1320, *et seq.*, a federal law designed to improve the efficiency and effectiveness of the American health care system. *See generally HIPAA for Professionals*, Health Information Privacy, https://www.hhs.gov/hipaa/for-professionals/index.html. In service of these objectives, HIPAA and its implementing regulations establish national standards to protect patients' medical records and individually identifiable health information ("IIHI"). Healthcare

[5] Plaintiff alleges that "upon information and belief, it is likely that the [Meta] Pixel was at one time running within the MyHealth Patient Portal as well." Compl. ¶ 105.

[6] Plaintiff alleges two alternative classes. The first is a Nationwide Class, defined as "[a]ll individuals residing in the United States who are, or were, patients of Defendant or any of its affiliates, used Defendant's [w]ebsite, and had their Private Information disclosed to a third party without authorization." The second is an Oregon Class, which would include only those patients residing in Oregon. *See* Compl. ¶¶ 172-73.

providers that conduct health care transactions electronically are required to limit the disclosure of PHI or face monetary penalties. *See* 45 C.F.R. Part 160 (2024).

The HIPAA Privacy Rule defines "PHI" and limits its disclosure. *See* 45 C.F.R. §§ 160.101-522, 164.102-106, 164.500-535 (2024). Pursuant to the Privacy Rule, PHI "means individually identifiable health information" that is "[t]ransmitted by electronic media; [m]aintained in electronic media; or [t]ransmitted or maintained in any other form or medium." 45 C.F.R. § 160.103. In turn, "IIHI" is defined as:

> [I]nformation that is a subset of health information, including demographic information collected from an individual, and:
>
> (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
>
> (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
>
> (i) That identifies the individual; or
>
> (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Id. The Privacy Rule forbids covered entities from disclosing PHI to third parties, with limited exceptions that are not relevant in this case. What *is* relevant to this case is that Plaintiff alleges that by installing tracking tools, Defendant impermissibly disclosed Plaintiff's PHI—specifically, her patient status and information taken from her medical records, patient web forms, and other online communication with her physicians. *See* Compl. ¶¶ 97-100.

DISCUSSION

A. First Claim: Breach of Confidence

To bring a claim for breach of confidence under Oregon common law, Plaintiff must allege an "unauthorized and unprivileged disclosure of confidential information obtained in a confidential relationship." *Humphers v. First Interstate Bank of Or.*, 298 Or. 706, 717 (1985). Further, the duty to maintain confidentiality must arise from a "legal source external to the tort claim itself." *A.B. v. Or. Clinic*, 321 Or. App. 60, 70 (2022) (quoting *Humphers*, 298 Or. at 719). Thus, the first step of a breach of confidentiality analysis is to identify this external legal source. Plaintiff claims that three independent external legal sources each create Defendant's duty to maintain the confidentiality of Plaintiff's PHI: HIPAA, Oregon Revised Statutes ("ORS") §§ 192.553-81 (which are analogous to HIPAA's protections), and the implied covenant of trust and confidence between a doctor and patient.

Defendant argues that because HIPAA and the comparable Oregon statutes lack a private right of action, Plaintiff cannot use them to establish that Defendant had a duty of confidentiality. The Court disagrees; that a statute does not authorize a private right of action does not mean that it cannot be used as an external legal hook for a tort claim. *See M.R. v. Salem Health Hosps. & Clinics*, 2024 WL 3970796, at *3-4 (D. Or. Aug. 28, 2024) (denying motion to dismiss an Oregon breach of confidence claim based on plausibly alleged violations of HIPAA through Google Analytics and Meta Pixel tracking data); *cf. A.B. v. Or. Clinic*, 321 Or. App. 60, 70 (2022) (analyzing an Oregon breach of confidence claim where the parties agreed that the duty of confidentiality arose from HIPAA and ORS §§ 192.553-81).

The Court agrees with Plaintiff that the two cited statutory sources provide for such a duty. *See, e.g.*, *M.R.*, 2024 WL 3970796, at *4 (concluding that healthcare provider sued by patient for breach of confidence had duty under HIPAA); *see also Humphers*, 298 Or. at 720 ("A

physician's duty to keep medical and related information in confidence is beyond question. It is imposed by statute."). Plaintiff also alleges, and Defendant does not dispute, that Plaintiff did not consent to any disclosure of medical information to Meta and Google.[7]

Having found an external duty to maintain the confidentiality of Plaintiff's PHI, the Court next asks whether Plaintiff has plausibly alleged that Defendant actually disclosed any of Plaintiff's information, and if so, whether that information was PHI. Because the Court sees a meaningful difference between searches conducted on a website accessible to anyone and a private portal provided to an individual patient, the Court separately analyzes Plaintiff's claims with respect to the Public Website and the Patient Portal.

Regarding the Public Website, Defendant argues that URL browsing data and search queries are not PHI. Plaintiff alleges in her complaint that she used the Public Website to search for burn specialists and burn treatments. The generic search queries created during such browsing activity, however, do not constitute PHI. *See Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 954-55 (N.D. Cal. 2017) (finding that searches for specific doctors and treatments on a healthcare provider's public website containing "general health information that is accessible to the public at large" did not constitute PHI under HIPAA) *aff'd*, 745 F. App'x 8 (9th Cir. 2018); *cf. R.C. v. Walgreen Co.*, 2024 WL 2263395, at *8 (N.D. Cal. May 9, 2024) (finding a plausible disclosure of PHI only where plaintiffs "allege[d] more than merely viewing generic medical content on a publicly facing website"). Accordingly, Plaintiff cannot proceed on her breach of confidence claim based on searches that she made on Defendant's Public Website.

[7] Specifically, Plaintiff cites Defendant's Notice of Privacy Practices (a page on its Public Website) ("NOPP") that allegedly lists the parties or entities to whom Defendant may disclose medical information—a list that does not include Google or Meta—and states that "[a]ll other uses and disclosures of medical information not covered by this notice or the laws that apply to us will be made *only with your written authorization*." Compl. ¶ 141 (emphasis by Plaintiff).

As for the Patient Portal, Defendant argues that Plaintiff has not explicitly alleged that any of her actual medical information was collected or transmitted (and, if transmitted, linked in any way to Plaintiff). First, the Court looks to whether Plaintiff adequately has alleged that Defendant transmitted information from the Patient Portal. Plaintiff alleges that she found Google Analytics on the landing page of her own Patient Portal, and Plaintiff includes screenshots in her complaint. Thus, Plaintiff adequately alleges that information was collected and transmitted from her Patient Portal. Drawing all reasonable inferences in Plaintiff's favor, as the Court must do at this stage of the litigation, the Court concludes that this tracking tool exists throughout the Patient Portal—even on pages beyond the landing page. It also is a reasonable inference that Google Analytics collects and transmits data from the pages within the Patient Portal on which it resides.

The Court next considers whether Plaintiff adequately has alleged that *PHI* was transmitted from the Patient Portal. Plaintiff alleges that Google Analytics was able to collect PHI that she and her Legacy Health providers disclosed on the Patient Portal. Plaintiff alleges that the compromised information on her Patient Portal included, among other things, her status as Defendant's patient, prescription information, and her specific treatment plans from her physical therapists.[8] Unlike search terms on a public website, patient status is PHI under HIPAA. *See Nienaber v. Overlake Hosp. Med.l Ctr.*, 2024 WL 2133709, at *3 (W.D. Wash., May 13, 2024) (stating, within a HIPAA framework, "[a]s other Courts within this Circuit have acknowledged, the transmission of information submitted to a *private patient portal*—such as a user clicking on the 'log in' button on that webpage—reveals patient status, which in and of

[8] The complaint states that Plaintiff's physical therapists sent her "links to YouTube for physical therapy *excises* for her burn wounds," which appears to be a typographical error for "*exercises*." Compl. ¶ 98 (emphasis added).

itself is protected health information."); *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 793 (N.D. Cal. 2022) (finding that "patient status is protected health information" under HIPAA); *M.R.*, 2024 WL 3970796, at *4 (finding that the plaintiff plausibly pled violations of HIPAA privacy requirements by alleging that the defendant's website's tracking tools revealed "the user's status as a patient and that the patient is seeking financial assistance").[9] So are other disclosures that Plaintiff made on her Patient Portal, including her treatment plans and prescriptions. *See* 45 C.F.R. § 160.103 (stating that PHI includes identifiable information relating to the "past, present, or future" health condition of an individual or the "provision of health care to an individual"). These allegations are sufficient to plead a claim of breach of confidence.[10]

Taking Plaintiff's allegations as true, Defendant disclosed Plaintiff's PHI from her Patient Portal without authorization to at least Google. Accordingly, with respect to disclosures from the Patient Portal, the Court denies Defendant's motion to dismiss on this claim.

---

[9] Defendant cites *Eisenhower Medical Center v. Superior Court*, 226 Cal. App. 4th 430, 436-37 (2014), to argue that patient status is not medical information. The court in that case, however, was analyzing a claim brought under the Confidentiality of Medical Information Act ("CMIA"), a California statute. *Id.* at 432. Indeed, the court reached its conclusion that patient status is not medical information by conducting a textual and structural analysis of CMIA. By contrast, Plaintiff in this case brings her claim under HIPAA—a different statute—and as noted, decisions by courts within this circuit have found that *under HIPAA*, patient status is PHI.

[10] Defendant argues that Plaintiff's complaint is too vague and conclusory with respect to disclosures made on the Patient Portal. To that end, Defendant analogizes to *B.K. v. Eisenhower Medical Center*, 721 F. Supp. 3d 1056 (C.D. Cal. 2024), in which the court dismissed a similar claim because the complaint was "replete with conjectures and hypothetical scenarios and patients" and "Plaintiffs fail to allege any specificity as to what medical information was allegedly disclosed or when it was disclosed." *Id.* at 1064. But Plaintiff pleads this claim with greater specificity than the *B.K. v. Eisenhower* plaintiffs. For example, Plaintiff provides in her complaint a screenshot of Google Analytics running on *her* Patient Portal (as opposed to the page of a hypothetical patient) and states with particularity that she received advertisements about the same medical conditions that were the subject of her activities on her portal. She further alleges that Defendant disclosed PHI including her status as a patient, health conditions, desired medical treatment, treatment plans from physical therapists, and prescriptions.

B. Second Claim: Violation of ECPA

ECPA authorizes a private right of action against any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a). Pursuant to the "party exception," however, "[i]t shall not be unlawful . . . for a person not acting under color of law to intercept a wire, oral, or electronic communication *where such person is a party to the communication*." 18 U.S.C. § 2511(2)(d) (emphasis added). Further, the party exception has its own carve-out: a party to a communication is still liable under ECPA when a communication "is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." *Id.*

Defendant argues that the party exception shields it from ECPA liability. Plaintiff responds that Defendant's alleged violation of HIPAA qualifies for the independent "criminal or tortious act" carve-out such that Defendant is still liable. Defendant replies that this carve-out does not apply because there was no independent criminal or tortious act beyond the alleged disclosure itself.

Courts around the country, including courts within this circuit, are divided on the issue of whether a HIPAA violation may constitute an independent crime under ECPA.[11] The Court

[11] *Compare, e.g.*, *M.R.*, 2024 WL 3970796, at *5 (Plaintiff "plausibly pled the crime/tort exception" by alleging HIPAA violations); *Cooper v. Mt. Sinai Health Sys.*, 2024 WL 3586357, at *7-9 (S.D.N.Y. July 30, 2024) (finding the same and collecting cases); *Murphy v. Thomas Jefferson Univ. Hosps., Inc.*, 2024 WL 4350328, at *4 (E.D. Penn. Sept. 30, 2024) (finding the same); *Mekhail v. N. Mem'l Health Care*, 2024 WL 1332260, at *4-5 (D. Minn. Mar. 28, 2024) (finding the same); *Kurowski v. Rush Sys. for Health*, 2023 WL 8544084, at *3 (N.D. Ill. Dec. 11, 2023) (finding that the transmission of the name of the plaintiff's physician and physician's specialty for financial gain was sufficient to trigger HIPAA and the exception carve-out); *with, e.g.*, *Okash v. Essentia Health*, 2024 WL 1285779, at *4 (D. Minn. Mar. 26, 2024) (holding that because "neither the alleged HIPAA nor privacy violations were independent of the interception, the crime-tort exception does not apply"); *Nienaber*, 2024 WL 2133709, at *15

agrees with the line of cases finding that violating HIPAA *can* constitute an independent criminal act for purposes of the carve-out to ECPA's party exception. This case involves not only the disclosure of private information, but also the disclosure of private *health* information as between a *healthcare provider and a patient*—which triggers HIPAA—for the unauthorized purpose of marketing services. Thus, the HIPAA violation is independent of the interception of Plaintiff's PHI.

The carve-out also applies because of Plaintiff's breach of confidence claim, which originates in tort. *Cf. R.C.*, 2024 WL 2263395, at *16 (finding that an invasion of privacy tort claim triggered the ECPA carve-out). Thus, finding that the carve-out to the "party exception" applies, the Court denies Defendant's motion to dismiss Plaintiff's ECPA claim. Because the carve-out is triggered either by a HIPAA violation or by a breach of confidence—both of which occur when a party discloses PHI—Plaintiff's ECPA claim may proceed only with respect to the Patient Portal, where she alleges that PHI was disclosed. As with her breach of confidence claim, this claim may not proceed with respect to alleged disclosures from the Public Website.

Defendant also argues that Plaintiff's ECPA claim fails because Plaintiff fails to allege that Defendant disclosed any PHI to a third party. For the same reasons that the Court found that Plaintiff sufficiently alleged transmission of PHI for Plaintiff's first claim, the Court finds that Plaintiff adequately has alleged disclosure under her second claim.

C. Third Claim: Invasion of Privacy (Intrusion Upon Seclusion)

To succeed on a claim intrusion upon seclusion claim under Oregon common law, a plaintiff must prove three elements: "(1) an intentional intrusion, physical or otherwise, (2) upon

---

(finding no sufficient distinction between the recording of communications and the transmission of those communications for the latter to constitute an independent crime).

the plaintiff's solitude or seclusion or private affairs or concerns, (3) which would be highly offensive to a reasonable person." *Mauri v. Smith*, 324 Or. 476, 483 (1996). The Court agrees with Plaintiff that she had a reasonable expectation of privacy with respect to her PHI that she or her providers disclosed on her Patient Portal. *See Doe I v. Google LLC*, 2023 WL 6882766, at *2 (N.D. Cal. Oct. 18, 2023) ("There is a reasonable expectation of privacy in one's private health information."). The Court also finds that disclosure of PHI would be highly offensive to a reasonable person. *See M.R.*, 2024 WL 3970796, at *6 ("Congress and courts have consistently noted that personal medical information is among the most sensitive information that could be collected about a person, and that the existence of many statutes like HIPAA and ORS § 192.553 regulating its disclosure supports this idea."); *Perez-Denison v. Kaiser Found. Health Plan of the Nw.*, 868 F. Supp. 2d 1065, 1090 (D. Or. 2012) ("HIPAA suggests Congress has determined reasonable people want their medical records private and strongly object to those records being inappropriately accessed."); *see also R.C.*, 2024 WL 2263395, at *9 (finding disclosure of PHI to be highly offensive where it involved medication and treatment related to specific health conditions).

The Court also finds, however, that Defendant's alleged conduct is not an intentional intrusion. Analyzing Oregon law, the Court concludes that Plaintiff's allegations fall short of an intentional intrusion. The leading case in analyzing this claim is *Humphers v. First Interstate Bank of Oregon*, 298 Or. 706 (1985). As the Oregon Supreme Court explained in *Humphers*, "[a]lthough claims of a breach of privacy and of wrongful disclosure of confidential information may seem very similar in a case like the present, which involves the disclosure of an intimate personal secret, the two claims depend on different premises and cover different ground." *Id.* at 711. The court concluded, where the defendant did not "pry into any personal facts that he did

not know," that "[t]he point of the claim against [the defendant] is not that he pried into a confidence *but that he failed to keep one*." *Id.* at 717 (emphasis added). Thus, the Oregon Supreme Court dismissed the invasion of privacy claim against the defendant.[12] Other courts, applying similar law, have held the same. *See, e.g.*, *Kurowski v. Rush Sys. for Health*, 683 F. Supp. 3d 836, 849 (N.D. Ill. 2023) ("Even drawing all inferences in Kurowski's favor, the only plausible conclusion the Court can arrive at is that the allegedly harmful intrusion here, if any, was accomplished by third parties. . . . [Defendant] cannot plausibly be considered to have intruded on, intercepted, or 'bugged' private communications that it was always the intended recipient of.").

Here, Plaintiff voluntarily accepted giving and receiving her PHI with Defendant on Defendant's website. Defendant was a party to Plaintiff's confidential data and its custodian, not an unknown accessor or pilferer of data. The problem is what Defendant then allegedly *did* with Plaintiff's PHI, which implicates Defendant's alleged duty to keep Plaintiff's information confidential. It is not an underlying intrusion on Plaintiff's seclusion. Thus, Plaintiff's allegations comport with a theory of breach of confidentiality (her first claim), not intrusion upon seclusion.[13] Accordingly, the Court dismisses this claim.

---

[12] Plaintiff cites cases that deny motions to dismiss on an intrusion upon seclusion claims, but most of those cases are not applying Oregon law. Plaintiff also cites *M.R.*, 2024 WL 3970796, at *5-6, as a supplemental authority, which allowed an intrusion upon seclusion claim to move forward under Oregon law. The Court, however, does not find the analysis in *M.R.* to be persuasive in analyzing this claim because *M.R.* did not address *Humphers* in reaching its conclusion.

[13] A relevant question is whether Plaintiff could have brought this claim under a different strand of the invasion of privacy tort, public disclosure of private facts. To bring such a claim, a plaintiff must show three elements: (1) the facts disclosed are private facts, (2) the defendant disclosed them to the public generally or to a large number of persons, and (3) the disclosure was in a "form of publicity of a highly objectionable kind." *Tollefson v. Price*, 247 Or. 398, 401-02 (1967). Plaintiff's allegations as pleaded in her complaint, however, also do not support a claim for public disclosure of private facts. The disclosure of private information to Google or Meta

D. Fourth Claim: Breach of Implied Contract

When parties manifest their agreement by words, the contract is said to be "express." When parties manifest an agreement by conduct, rather than by words, the contract is said to be "implied in fact." The method of manifesting agreement—by words or conduct—is the only material difference between an express and an implied-in-fact contract. In all other respects, an implied-in-fact contract is treated as any other contract, and "must be founded upon the mutual agreement and intention of the parties." *Moyer v. Columbia State Bank*, 315 Or. App. 728, 737 (2021) (quotation marks omitted).

Plaintiff alleges that she provided Defendant with her PHI as a condition of using the Patient Portal and receiving services from Defendant's healthcare professionals. She alleges that after she began providing this PHI, she and Defendant "entered into an implied contract pursuant to which Defendant agreed to safeguard and not disclose [her] Private Information without consent," Compl. ¶ 251, which Defendant then breached. Plaintiff further alleges that Defendant's Notice of Privacy Practices ("NOPP") was the source upon which she understood there to be mutual assent.

The Court disagrees with Plaintiff and finds that Plaintiff has not sufficiently alleged the existence of an implied-in-fact contract. "A patient's choice to use Defendant as a medical service provider does not indicate an intention to enter into an implied contract for the security of

---

with the result of *Plaintiff* (and not the general public) seeing that information in the form of targeted advertising, is not disclosure "to the public generally or to a large number of persons." *Cf. Nienaber*, 2024 WL 2133709, at *10 (dismissing a public disclosure claim under Washington law because "Plaintiff does not allege that the information shared by Defendant will become available to the public *at large*; to the contrary, Plaintiff alleges that the information is shared with Facebook, and in turn, being used by Facebook to target Plaintiff herself" (emphasis in original)); *Kurowski*, 683 F. Supp. 3d at 849-50 (dismissing a public disclosure claim under Illinois law because the "only disclosures allegedly made were to Facebook, Google, and/or Bidtellect, which are private companies," and not "the public at large").

information entered on Defendant's website." *M.R.*, 2024 WL 3970796, at *6. Furthermore, Plaintiff's reference to Defendant's NOPP as the source of mutual assent is misplaced because she never alleges that she relied upon or even read the NOPP before engaging Defendant's services. *Cf. Gay v. Garnet Health*, 2024 WL 4203263, at *6 (S.D.N.Y. Sept. 16, 2024) (finding no mutual assent because the plaintiffs did not allege that they viewed the defendant's privacy policy, the basis of their implied contract claim, before engaging the defendant's services). Because Plaintiff has not shown mutual assent, she has not sufficiently pleaded the existence of an implied-in-fact contract—and thus the breach of one. The Court grants Defendant's motion to dismiss as to this claim.[14]

E. Fifth Claim: Unjust Enrichment

To establish a claim for unjust enrichment under Oregon law, Plaintiff must show: "(1) a benefit conferred, (2) awareness by the recipient that she has received the benefit, and (3) it would be unjust to allow the recipient to retain the benefit without requiring her to pay for it." *Cron v. Zimmer*, 255 Or. App. 114, 130 (2013); *see also Larisa's Home Care, LLC v. Nichols-Shields*, 362 Or. 115, 124-31 (2017) (discussing Oregon's unjust enrichment framework). Plaintiff alleges that because Defendant collected and disclosed Plaintiff's private data to

[14] The Court further notes that although Plaintiff brought a breach of contract claim based on an implied-in-fact contract, the real breach may have been founded in an *express* contract. Plaintiff alleges that "[*a*]*s a condition* of utilizing Defendant's Website and receiving services from Defendant's healthcare facilities and professionals, Plaintiff and the Class Members provided their Private Information and compensation for their medical care." Compl. ¶ 250 (emphasis added). That Plaintiff was already a patient of Defendant, had a Patient Portal on Defendant's website, and was compensating Defendant for medical services suggests that there may have already been an express contract—or a series of express contracts—between the parties. Therefore, it may be more appropriate to handle a claim alleging Defendant's obligation to safeguard PHI not as a breach of an implied *contract*, but rather as a breach of an implied *term* in an express contract. Because Plaintiff does not allege the existence of an express contract, however, the Court simply dismisses her claim as pleaded.

Defendant's monetary benefit, those benefits should be disgorged to Plaintiff (and the putative class).

Defendant first argues that an unjust enrichment claim is improper when other causes of action would provide adequate remedies at law. On this point, Defendant is correct; equitable remedies are appropriate only when there is no adequate remedy of law—that is, when there is no "practical, efficient, and adequate" solution in the law. *Martell v. Gen. Motors LLC*, 492 F. Supp. 3d 1131, 1148 (D. Or. 2020). Rule 8(d) of the Federal Rules of Civil Procedure, however, permits parties at this stage of litigation to plead various claims in the alternative. That is what Plaintiff has done here. Although it is possible that monetary damages as a remedy at law may be adequate, it would be premature to make that determination at the motion to dismiss stage. *See id.* ("At this stage of the litigation, it is unknown whether the remedy at law meets this standard.").[15] Accordingly, the Court will not dismiss this claim at this stage on this ground.

Defendant next argues that Plaintiff fails to explain how she has lost value in her PHI as a result of the alleged disclosure, and thus that it is inequitable for Defendant to keep the alleged benefit. Plaintiff alleges that her PHI was beneficial to Defendant because it provided Defendant with "economic, intangible, and other benefits, including substantial monetary compensation." Plaintiff further alleges that Defendant "consciously" disclosed this information to third parties for its own benefit, without compensating or seeking authorization from Plaintiff. That Plaintiff's medical information did not necessarily lose value as a result Defendant's alleged disclosure

[15] Defendant argues that Plaintiff's reliance on *Martell* is inappropriate because "[a]ny benefit conferred upon *Legacy Health* (which is none) has already been alleged and can be assessed at the pleading stage." The Court disagrees. Without any discovery—for example, about the full range of disclosures, the duration of disclosures, and any contractual arrangement between Defendant and third parties to install tracking tools on Defendant's website—determining the full extent of the benefit at this stage would be premature.

does *not* necessarily foreclose her unjust enrichment claim. The key question is whether a benefit was conferred to Defendant and as between Plaintiff and Defendant, it is more unjust for the benefit to stay with Defendant without payment to Plaintiff (and the putative class). *See In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 599-600 (9th Cir. 2020) (concluding that the plaintiffs adequately alleged an unjust enrichment claim under California law even where the plaintiff did not suffer a corresponding loss because, under the circumstances, as between the plaintiffs and Facebook, it was adequately alleged that it was unjust for Facebook to retain profits from the plaintiffs' personal data). Accordingly, at this stage of the litigation, the Court denies the motion to dismiss insofar as this claim concerns disclosure of PHI on the Patient Portal.

F. Sixth Claim: Negligence

Generally, a negligence claim brought under Oregon law requires a plaintiff to show that a defendant's conduct "unreasonably created a foreseeable risk to a protected interest of the kind of harm that befell the plaintiff." *Fazzolari v. Portland Sch. Dist. No. 1J*, 303 Or. 1, 17 (1987). "'Duty' is not an element of a negligence case unless the claim involves an obligation arising from a special relationship which creates, limits or defines the obligation." *Budd v. Am. Sav. & Loan Ass'n*, 89 Or. App. 609, 612 (1988). When this type of special relationship between the tortfeasor and injured party exists, the former owes the latter "a duty to exercise reasonable care beyond the common law duty to prevent foreseeable harm." *Conway v. Pac. Univ.*, 324 Or. 231, 239 (1996).

Defendant first argues that it owed Plaintiff no special duty to safeguard her PHI. The Court disagrees. Both Oregon common law and HIPAA find a special relationship between physicians and their patients. *See id.*; *R.C.*, 2024 WL 2263395, at *11 (finding that HIPAA could form the basis of a California negligence claim against a healthcare provider under similar facts

even though HIPAA does not itself contain a private right of action).[16] Part of the special relationship between a physician and patient is the understanding that a patient's medical information will be kept confidential. *See Booth v. Tektronix, Inc.*, 312 Or. 463, 472 (1991) (summarizing the various sources imposing confidentiality in a physician-patient relationship, including the Hippocratic Oath and Oregon state law). Plaintiff thus sufficiently alleges that as her healthcare provider, Defendant owed her a duty to exercise reasonable care to protect her PHI—including, but not limited to, her patient status, health conditions, and treatments—with respect to anything she disclosed on the Patient Portal.

Defendant next argues that Plaintiff fails adequately to show a breach because Plaintiff fails to allege any protected information was disclosed. The Court already has rejected this argument at this stage of the litigation. Defendant also argues that Plaintiff fails to allege a link between the alleged disclosure and the alleged harm—targeted advertising. Specifically, Defendant argues that "Plaintiff's alleged receipt of advertisements regarding her medical conditions after visiting Legacy Health's public website falls far short of plausibly alleging that Legacy Health's alleged breach of a duty was the cause (as opposed to Plaintiff's general Internet use or browsing activities on other websites)." Plaintiff's allegations, however, differ in two important ways. First, Plaintiff alleges that information from both the public *and private*

[16] Defendant urges the Court to distinguish between "a classically recognized, special relationship directly between a physician and patient" and the relationship at issue in this case, which Defendant characterizes as "the relationship between a non-profit hospital system acting as a website operator and a website visitor who may (or may not) be a patient." At this stage, the Court declines to make this distinction. Advances in technology have caused the healthcare industry to shift rapidly in recent years. With services such as virtual appointments and the ability to chat directly with or message health-related questions to doctors online, a patient's private portal in many ways is a virtual locus of the hospital itself. That Plaintiff allegedly disclosed PHI online as opposed to in a physical office does not necessarily diminish Defendant's duty as Plaintiff's healthcare provider to safeguard her PHI.

faces of the website contributed to the targeted advertising. Second, Plaintiff explicitly alleges that she did *not* disclose any PHI to any other source. Compl. ¶ 112 ("Plaintiff did not disclose this Private Information to any other source—only to Defendant's Website.").[17] Therefore, accepting Plaintiff's allegations as true and construing the facts in the light most favorable to Plaintiff, the Court finds that she sufficiently has linked the targeted advertising to—at least in part—information that Plaintiff disclosed on her Patient Portal.

Finally, Defendant argues that Plaintiff has not adequately pleaded damages. Defendant asserts that Plaintiff fails to "plead facts showing that she lost the opportunity to sell her information or that the value of her information was somehow diminished after it was allegedly collected by Meta or Google."[18]

Defendant argues that Plaintiff must allege that there is a market for her PHI and that Plaintiff herself intended to use that market. Defendant cites *C.M. v. MarinHealth Med. Grp., Inc.*, 2024 WL 217841, at *2 (N.D. Cal. Jan. 19, 2024), which was relying on the judge's earlier opinion analyzing California's Unfair Competition Law. This case is not persuasive.

[17] Plaintiff's counsel confirmed this allegation during oral arguments.

[18] Plaintiff alleges nine theories of damages in her negligence claim, but Defendant only challenges Plaintiff's diminution-in-value theory of damages, and thus the Court only discusses this theory of damages. The Court notes, however, that even if Defendant were correct that Plaintiff's diminution-in-value theory of damages was insufficiently alleged, that says nothing about Plaintiff's other, unchallenged theories, such as Plaintiff's invasion of privacy theory of damages. *See, e.g.*, *In re Facebook*, 956 F.3d at 599 ("Here, Plaintiffs have adequately alleged that Facebook's tracking and collection practices would cause harm or a material risk of harm to their interest in controlling their personal information."); *Doe v. Tenet Healthcare Corp.*, 2024 WL 1756075, at *3 (D. Mass. Apr. 23, 2024) (denying motion to dismiss negligence claim under Massachusetts law and accepting as adequately pled damages of "her Private Information—including her identity, patient status, and her health conditions and treatments—[having been] collected and transmitted to Facebook and third parties without her consent").

Defendant cites no appellate authority holding that a plaintiff who alleges the dissemination of personal data must also allege that she herself would have participated in a market to sell her own confidential data. Indeed, many district courts in this circuit have rejected this theory and the Court agrees. *See, e.g.*, *In re Anthem, Inc. Data Breach Litig.*, 2016 WL 3029783, at *15 (N.D. Cal. May 27, 2016) (reviewing cases and concluding that plaintiffs "are not required to plead that there was a market for their PII [personally identifiable information] *and* that they somehow also intended to sell their own PII" because the cases instead "require a plaintiff to allege that there was either an economic market for their PII *or* that it would be harder to sell their own PII, not both" (emphases in original)); *Smallman v. MGM Resorts Int'l*, 638 F. Supp. 3d 1175, 1190 (D. Nev. 2022) (concluding that "these pleading requirements, that Plaintiffs must establish both the existence of a market for their PII and an impairment of their ability to participate in that market, is not supported by Ninth Circuit precedent and other district courts in this Circuit have rejected them" (gathering cases)); *but see R.C.*, 2024 WL 2263395 ("Here, the case concerns the receipt of personal health information which Plaintiffs consider too private to share with third parties. As such, it is unclear 'how plaintiffs could and would participate in a legitimate market for health care information.'" (quoting *Doe v. Meta Platforms, Inc.*, --- F. Supp. 3d at ---, 2023 WL 5837443, at *15 (N.D. Cal. Sept. 7, 2023))).

At this stage of the litigation, particularly given that this case involves the relatively new area of tracking tools placed on health care websites, the Court finds that Plaintiff has sufficiently alleged enough facts relating to diminution in value to survive a Rule 12(b)(6) motion. Whether, after further development of facts, Plaintiff can meet her burden of production at summary judgment or at trial is a question for another day.

As a final point, the Court acknowledges that Plaintiff's negligence claim rests on the same facts as her breach of confidence claim. "Courts in this District consistently reject negligence claims at the summary judgment stage when the negligence claim is based on the same facts as . . . an intentional tort." *Wagoner v. City of Portland*, 2017 WL 2369399, at *11 (D. Or. May 31, 2017) (collecting cases). At this early stage of the litigation, however, "Rule 8 [of the Federal Rules of Civil Procedure] permits an allegation of negligence in one count and an allegation of intentional action, based on the same facts, in another." *Rodriguez v. City of Portland*, 2009 WL 3518004, at *2 (D. Or. Oct. 21, 2009). Accordingly, the Court allows this claim to proceed, but again, only as it pertains to activity on the Patient Portal.

CONCLUSION

The Court grants in part and denies in part Defendant's Motion to Dismiss (ECF 20). The Court grants the motion as to Plaintiff's third claim (invasion of privacy) and fourth claim (breach of implied contract). The Court also grants the motion with respect to Plaintiff's first (breach of confidence), second (ECPA), fifth (unjust enrichment), and sixth (negligence) claims insofar as they concern activities on Defendant's Public Website. The Court denies the motion with respect to Plaintiff's first, second, fifth, and sixth claims insofar as these claims concern activities on Defendant's Patient Portal.

IT IS SO ORDERED.

DATED this 14th day of November, 2024.

/s/ *Michael H. Simon*
Michael H. Simon
United States District Judge